

S12500-X交换机包过滤优化经验案例

一、组网图：

无

二、组网需求：

在12500-X交换机EA、EB、EC类业务单板上部署包过滤功能。如果包过滤规则需要部署到大量虚接口时，受单板ACL规格数限制，可能存在资源不足，导致PBR无法正常生效问题。

下面通过对比包过滤ACL规则下发在设备物理接口、虚接口时，对比设备ACL资源占用情况，了解12500-X交换机包过滤占用设备ACL资源的规则。同时通过举例，了解当ACL规则内容新增时，12500-X设备ACL资源占增加的情况。

三、关键配置：

在物理接口上部署包过滤规则配置：

创建包过滤规则ACL，其中包括5个RULE

```
#
acl number 3001 name Packet-filter

rule 10 deny ip source 10.1.1.1 0 destination 172.16.1.1 0

rule 20 deny ip source 10.1.1.2 0 destination 172.16.1.1 0

rule 30 deny ip source 10.1.1.3 0 destination 172.16.1.1 0

rule 40 deny ip source 10.1.1.4 0 destination 172.16.1.1 0

rule 50 deny tcp destination-port eq telnet
```

#

将包过滤规则下发到3个物理接口上

#

```
interface Ten-GigabitEthernet1/0/1

port link-mode bridge

port access vlan 131

packet-filter 3001 inbound
```

#

```
interface Ten-GigabitEthernet1/0/2

port link-mode bridge

port access vlan 131

packet-filter 3001 inbound
```

#

```
interface Ten-GigabitEthernet1/0/3

port link-mode bridge

port access vlan 131

packet-filter 3001 inbound
```

#

通过display qos-acl resource命令观察，此时设备ACL IFP占用的资源为5条，如下：

Type	Total	Reserved	Configured	Remaining	Usage
VFP ACL	2048	1024	0	1024	50%

IFP ACL	8192	2048	5	6139	25%
IFP Meter	4096	1024	0	3072	25%
IFP Counter	4096	1024	0	3072	25%
EFP ACL	1024	0	0	1024	0%
EFP Meter	512	0	0	512	0%
EFP Counter	512	0	0	512	0%

包过滤规则部署在物理接口inbound方向后，对于进入接口的流量匹配动作，因此将占用IFP资源（入方向资源）。12500-X设备ACL资源定义，对于包过滤规则下发在物理接口入方向占用IFP公式为，IFP占用数 = RULE数量。因此上面举例中RULE数量等于5条，下发到了3个物理接口上，IFP占用数= 5条。包过滤规则部署在物理接口inbound方向，不会随着部署的物理接口数增加而导致占用ACL IFP资源增加。

在虚接口上部署包过滤规则配置：

创建包过滤规则ACL，其中包括5个RULE

```
#
acl number 3002 name Packet-filter

rule 10 deny ip source 10.1.1.1 0 destination 172.16.1.1 0
rule 20 deny ip source 10.1.1.2 0 destination 172.16.1.1 0
rule 30 deny ip source 10.1.1.3 0 destination 172.16.1.1 0
rule 40 deny ip source 10.1.1.4 0 destination 172.16.1.1 0
rule 50 deny tcp destination-port eq telnet
```

将包过滤规则下发到3个虚接口上

```
#
interface Vlan-interface1111
ip address 11.35.11.254 255.255.255.0
packet-filter 3002 inbound

#
interface Vlan-interface1112
ip address 11.35.12.254 255.255.255.0
packet-filter 3002 inbound

#
interface Vlan-interface1113
ip address 11.35.13.254 255.255.255.0
packet-filter 3002 inbound
```

此时通过display qos-acl resource命令观察，当把ACL下发在3个虚接口上后，设备ACL IFP资源将占用15条。如下：

Type	Total	Reserved	Configured	Remaining	Usage
VFP ACL	2048	1024	0	1019	50%
IFP ACL	8192	2048	15	6129	26%
IFP Meter	4096	1024	0	3072	25%
IFP Counter	4096	1024	0	3072	25%
EFP ACL	1024	0	0	1024	0%
EFP Meter	512	0	0	512	0%
EFP Counter	512	0	0	512	0%

包过滤规则部署在虚接口inbound方向后，对于进入接口的流量匹配动作，因此将占用

FP资源（入方向资源）。12500-X设备ACL资源定义，对于包过滤规则下发在虚接口入方向占用IFP公式为，IFP占用数 = SVI数量 * RULE数量。因此上面举例中RULE数量等于5条，下发到了3个SVI接口上，IFP占用数= 5 * 3 = 15条。

在物理接口、虚接口同时部署包过滤规则后，增加新类型规则配置：

创建包过滤规则ACL 3001，其中包括5个RULE

```
#
acl number 3001 name 3001

rule 10 deny ip source 10.1.1.1 0 destination 172.16.1.1 0

rule 20 deny ip source 10.1.1.2 0 destination 172.16.1.1 0

rule 30 deny ip source 10.1.1.3 0 destination 172.16.1.1 0

rule 40 deny ip source 10.1.1.4 0 destination 172.16.1.1 0

rule 50 deny tcp destination-port eq telnet
```

```
#
创建包过滤规则ACL 3002，其中包括5个RULE
```

```
#
acl number 3002 name 3002

rule 10 deny ip source 10.1.1.1 0 destination 172.16.1.1 0

rule 20 deny ip source 10.1.1.2 0 destination 172.16.1.1 0

rule 30 deny ip source 10.1.1.3 0 destination 172.16.1.1 0

rule 40 deny ip source 10.1.1.4 0 destination 172.16.1.1 0

rule 50 deny tcp destination-port eq telnet
```

```
#
将ACL 3001部署在3个物理接口上；同时将ACL 3002部署在3个虚接口上
```

```
#
interface Ten-GigabitEthernet1/0/1

port link-mode bridge

port access vlan 131

packet-filter 3001 inbound

#
interface Ten-GigabitEthernet1/0/2

port link-mode bridge

port access vlan 131

packet-filter 3001 inbound

#
interface Ten-GigabitEthernet1/0/3

port link-mode bridge

port access vlan 131

packet-filter 3001 inbound

#
interface Vlan-interface1111

ip address 11.35.11.254 255.255.255.0

packet-filter 3002 inbound

#
interface Vlan-interface1112

ip address 11.35.12.254 255.255.255.0

packet-filter 3002 inbound

#
```

```
interface Vlan-interface1113

ip address 11.35.13.254 255.255.255.0

packet-filter 3002 inbound

#
```

根据前面包过滤ACL占用资源规则，当前占用设备ACL IFP资源数量为20条（下发在3个物理接口上的规则占用5条，下发在3个虚接口上的规则占用15条）

Type	Total	Reserved	Configured	Remaining	Usage
VFP ACL	2048	1024	0	1019	50%
IFP ACL	8192	2048	20	6129	26%
IFP Meter	4096	1024	0	3072	25%
IFP Counter	4096	1024	0	3072	25%
EFP ACL	1024	0	0	1024	0%
EFP Meter	512	0	0	512	0%
EFP Counter	512	0	0	512	0%

在此情况下，在ACL 3001中新增RULE 60，且RULE 60 匹配类型为port range，如下：

```
#

acl number 3001 name 3001

rule 10 deny ip source 10.1.1.1 0 destination 172.16.1.1 0

rule 20 deny ip source 10.1.1.2 0 destination 172.16.1.1 0

rule 30 deny ip source 10.1.1.3 0 destination 172.16.1.1 0

rule 40 deny ip source 10.1.1.4 0 destination 172.16.1.1 0

rule 50 deny tcp destination-port eq telnet

rule 60 deny tcp destination-port range 100 1024

#
```

新增rule 60规则之后，通过display qos-acl resource命令观察，此时设备ACL IFP占用的资源为42条，如下：

Type	Total	Reserved	Configured	Remaining	Usage
VFP ACL	2048	1024	0	1024	50%
IFP ACL	8192	2048	42	6102	26%
IFP Meter	4096	1024	0	3072	25%
IFP Counter	4096	1024	0	3072	25%
EFP ACL	1024	0	0	1024	0%
EFP Meter	512	0	0	512	0%
EFP Counter	512	0	0	512	0%

包过滤规则部署在接口inbound方向后，12500-X设备ACL资源定义，如果rule规则中包含port-range规则，那么将会把整个包过滤规则占用数量*2，及IFP占用数 = （物理课RULE数量 + SVI数量 * RULE数量）*2。因此上面举例中下发在物理接口入方向RULE数量等于6条，下发到了3个SVI接口上的RULE数量等于5，IFP占用数=（6 + 3*5）* 2 = 42条。

以上述配置为例，对于port-range规则的包过滤，建议将其单独下发在物理口outboard方向，从而减少对于ACL IFP资源的占用，具体配置如下：

```
#

acl number 3001 name 3001

rule 10 deny ip source 10.1.1.1 0 destination 172.16.1.1 0

rule 20 deny ip source 10.1.1.2 0 destination 172.16.1.1 0
```

```

rule 30 deny ip source 10.1.1.3 0 destination 172.16.1.1 0
rule 40 deny ip source 10.1.1.4 0 destination 172.16.1.1 0
rule 50 deny tcp destination-port eq telnet

#
acl number 3002 name 3002
rule 10 deny ip source 10.1.1.1 0 destination 172.16.1.1 0
rule 20 deny ip source 10.1.1.2 0 destination 172.16.1.1 0
rule 30 deny ip source 10.1.1.3 0 destination 172.16.1.1 0
rule 40 deny ip source 10.1.1.4 0 destination 172.16.1.1 0
rule 50 deny tcp destination-port eq telnet

#
acl number 3003 name 3003
rule 60 deny tcp destination-port range 100 1024

#
interface Ten-GigabitEthernet1/0/1
port link-mode bridge
port access vlan 131
packet-filter 3001 inbound
packet-filter 3003 outbound

#
interface Ten-GigabitEthernet1/0/2
port link-mode bridge
port access vlan 131
packet-filter 3001 inbound
packet-filter 3003 outbound

#
interface Ten-GigabitEthernet1/0/3
port link-mode bridge
port access vlan 131
packet-filter 3001 inbound
packet-filter 3003 outbound

#
interface Vlan-interface1111
ip address 11.35.11.254 255.255.255.0
packet-filter 3002 inbound

#
interface Vlan-interface1112
ip address 11.35.12.254 255.255.255.0
packet-filter 3002 inbound

#
interface Vlan-interface1113
ip address 11.35.13.254 255.255.255.0
packet-filter 3002 inbound

#

```

当RULE 60规则下发到物理接口outbound方向时，将不再使ACL IFP资源剩2，RULE 60规则仅占用1条 ACL EFP资源（outbound方向资源）

Type	Total	Reserved	Configured	Remaining	Usage

VFP ACL	2048	1024	0	1024	50%
IFP ACL	8192	2048	20	6124	26%
IFP Meter	4096	1024	0	3072	25%
IFP Counter	4096	1024	0	3072	25%
EFP ACL	1024	0	1	1024	0%
EFP Meter	512	0	0	512	0%
EFP Counter	512	0	0	512	0%

四、 总结

12500-X交换机，对于包过滤过账下发在物理接口/虚接口上时，ACL占用公式如下：

物理接口时，ACL占用量 = RULE数量；

虚接口时，ACL占用量 = RULE数量 * SVI接口数量。

当12500-X交换机，一个包过滤中同时存在非port-range RULE规则和port-range RULE规则时，建议将规则拆分。通过创建两个ACL，将其下发在接口的不同方向方式，进而达到优化资源的目的。